451 Research | Business Impact Brief

Email security: the biggest problem you're not paying attention to

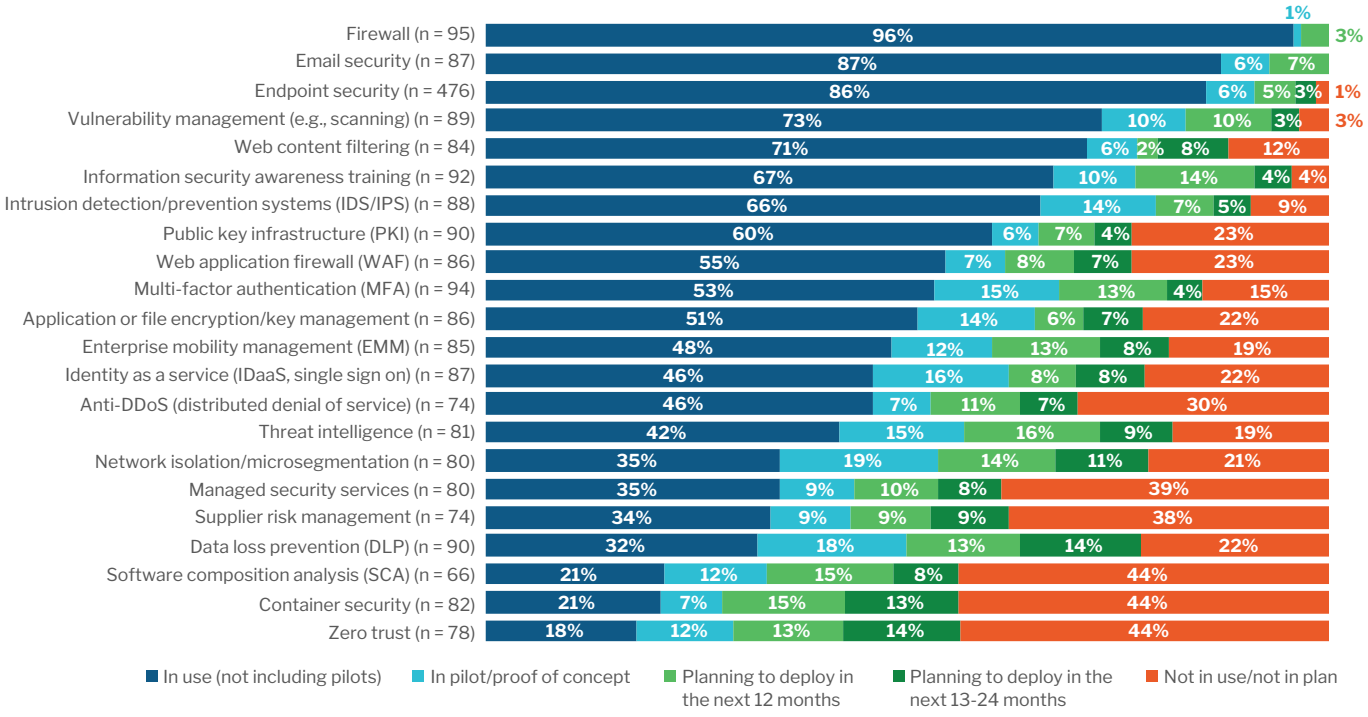
The 451 Take

On the surface, email security would appear to be a solved problem. Email security tools have been around for years, and according to survey data from 451 Research's Voice of the Enterprise (VotE) service, nearly nine out of 10 organizations (87%) have email security products already deployed, second only to firewalls (95%). Paradoxically, additional VoTE survey data shows that email (46%) poses the greatest data threat – by a wide margin. Nearly half of respondents (46%) cite email as the biggest vulnerability, a nearly fivefold lead over the next-greatest concerns – web browsing (10%) and internal networks (10%).

Also, user behavior (28%) and phishing (24%) – both highly correlated with email security – are listed as the top two pain points for security managers (24%), yet phishing is not among the top 10 strategic objectives for CISOs, according to 451 data, indicating they are not investing sufficiently in the problem. No surprise, then, that the Verizon DBIR data shows that 91% of breaches are email-related.

Organizations' Implementation Status for Various Technologies

Source: 451 Research's VotE: Information Security, Workloads & Key Projects, Q1 2019



Why? One reason is that email is still nearly ubiquitous. Certainly, apps like OneDrive, Dropbox, Google Drive and Slack make it easier to collaborate and share files, but for most enterprises, email remains the primary way employees communicate and share data. Furthermore, email-based threats adapt very rapidly, and like other areas of security, email security is essentially an arms race between the 'bad guys' and the 'good guys' who are constantly trying to keep up.

451 Research | Business Impact Brief

The 451 Take (continued)

The main point is that there is clearly a massive disconnect: if most firms have email security in place, yet email is still the number one threat, then clearly email security is *not* a solved problem. Yet only 7% plan to invest in email security in the next 12 months, compared to emerging categories such as container security (28%), zero trust (27%) and micro-segmentation (25%) – suggesting most firms are underinvesting in email protection.

We need a new way to solve the email security problem.

Business Impact

NATIVE CLOUD SECURITY IS NOT ENOUGH. Microsoft, AWS, Google and other cloud providers are constantly adding new security features and functionality, but the default offerings are targeted by threat actors, carry high false positives, and are provided on a 'best effort' basis from cloud vendors. 451 Research VoTE data shows that nearly half of all firms (~48%) are taking advantage of independent, third-party security offerings to fully optimize their security instead of relying solely on what the cloud providers offer.

BUSINESS RISKS. As the front door to corporate infrastructure, email and associated workplace collaboration solutions like Microsoft Office 365 and G Suite must be hardened to combat evolving threats from attackers at home and abroad. Data loss, reputational risk and other factors can present an unrecoverable barrier for organizations, especially smaller ones. Data breaches also lead to a breach in reputation and trust among partners and clients.

COST FACTORS. Email security vulnerabilities that lead to business email compromises cost millions annually. Cyber-insurance premiums, direct payments such as ransomware, and other losses such as those from fake invoice scams take real dollars from the bottom line. In addition, email security incident response, which pulls valuable resources from security operations centers – represents a hefty human capital cost.

USERS AREN'T PERFECT. The importance of user awareness training (UAT) has been highlighted in recent years, but UAT still has drawbacks, including taking valuable time away from busy users. Most importantly, no matter how much they are trained, users are not perfect, and it only takes one effective email compromise to cause a massive breach. The best phishing or malware attack is one that users never see.

Looking Ahead

Supplemental solutions should add to – not replace – default security layers. This ensures that the basic filtering (spam/graymail) as well as new attack signatures are constantly updated, while advanced threat software addresses evolving and zero-day attacks. It's also important to scan all email traffic. Traditional email gateways require complex configurations to detect internal email, which is frequently used to phish other business users in account-takeover attacks. Conversely, external emails can use spoofing and other evasion techniques that email gateways might also miss.

Attacks designed to trick humans should rely on machine learning and artificial intelligence (AI) capabilities. These include natural language processing, identification of key indicators of compromise, and multifaceted attacks that thread pin-hold vulnerabilities in known security layers. These necessarily can't rely on static/deterministic algorithms, so as to avoid false positives.

Proxies and cloud access security brokers (CASBs) are a common choice for many web, cloud and email security use cases, but proxy-based CASBs can present challenges for both admins and your own employees – and bad guys will typically bypass them. APIs present an alternative to slower proxy-based solutions, but the majority don't offer real-time responses and can only quarantine malicious content after delivery and a brief incubation period. An inline API that scans for emails inside the cloud before they arrive at the inbox offers the best of both worlds and brings the concept of perimeter security to each inbox.

AVANAN

PATENTED INLINE EMAIL SECURITY VIA API FROM AVANAN

Avanan pioneered a new approach to prevent sophisticated email attacks, using APIs to block phishing, malware and data leakage in the line of communications traffic. This means the platform catches threats missed with existing security, while adding a transparent layer of security for the entire collaboration suites like Microsoft Office 365 that also addresses security concerns across workplace collaboration software tools such as Slack. They have over 1,000 clients, ranging from small businesses to 250,000+ user global enterprises.